IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

SARAH E. RICHARDS, *individually and on behalf of all others similarly situated*, Plaintiff, v. **HCA HEALTHCARE, INC.,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Sarah E. Richards ("Plaintiff") brings this Class Action Complaint, individually on behalf of herself and on behalf of all others similarly situated (the "Class Members"), against Defendant HCA Healthcare, Inc. ("HCA" or "Defendant") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated personal data from HCA's systems that resulted in unauthorized access to the highly-sensitive data[1] of Plaintiff, and, according to Defendant, at least 11 million Class Members[2] ("Data Breach").[3] The data exposed is made up of approximately 27 million rows of patient information, and includes patients' personal information

[1] HCA Healthcare Reports Data Security Incident," https://hcahealthcare.com/about/privacy-update.dot (last viewed September 11, 2023).
[2] HCA Healthcare said the personal data of about 11 million patients in 20 states may have been stolen in a data breach. Samples of the data, including addresses, phone numbers, emails and birth dates, were posted to an online forum popular with cybercrooks by a hacker trying to sell them. The hacker purportedly claimed to have 27.7 million records. *See* https://fortune.com/2023/07/12/medical-giant-hca-healthcare-personal-data-11-million-patients-20-states-stolen-data-breach/ (last viewed September 15, 2023).
[3] *Id.*

and certain visit records.[4]

2. As presented on its website, HCA is "one of the nation leading providers of healthcare services, HCA Healthcare is comprised of 182 hospitals and 2,300+ sites of care in 20 states and the United Kingdom. In addition to hospitals, sites of care include surgier centers, freestanding ERs, urgent care centers, diagnostic and imaging centers, walk-in clinics and physician clinics."[5]

3. Founded in 1968, HCA boasts that "[m]any things set HCA Healthcare apart from other healthcare organizations; however at our core, our greatest strength is our people. Every day, more than 290,000 colleagues go to work with a collective focus: our patients." HCA goes on to state, that "[A]s a learning health system, HCA Healthcare analyzes data from more than 37 million patient encounters each year. This data helps develop technologies and best practices that improve patient care."[6] (Emphasis added.)

4. Despite its vast experience as a healthcare provider, HCA did not protect the personally identifying information ("PII") and the protected health information ("PHI") of their patients—the Class Members.[7]

5. Even if stolen PII or PHI does not include financial or credit card payment account information, that does not mean there has been no harm to the victims of the breach, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as

[4] *See* 2023 HCA Website, Substitute Notice, https://hcahealthcare.com/util/documents/2023/SubstituteNotice.pdf (last viewed September 17, 2023).
[5] *Id*. 2023 HCA Website, https://hcahealthcare.com/about/ (last viewed September 17, 2023).
[6] *Id*.
[7] PII and PHI are referred to jointly and collectively throughout this Complaint as "Private Information" and contains information such as names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer identification numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names).

social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

6. Based on the value of its patients' PII and PHI to cybercriminals, HCA knew or should have known the importance of safeguarding the PII and PHI entrusted to it and of the foreseeable consequences if its data security systems were breached. HCA failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

7. Defendant maintained Class Members' Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and as such Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that Private Information in a vulnerable condition.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, and giving false information to police during an arrest.

9. The data exposed in the Data Breach has already been made available for sale by the hacker, who posted a sample of the stolen data online on July 5, 2023.[8]

10. As a result of the Data Breach and exposure of their PII and PHI online, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

11. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct and asserting claims for: (i) negligence; (ii) breach of express contract; (iii) breach of implied contract; (iv) unjust enrichment; (v) bailment; and (vi) breach of fiduciary duty. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

[8] *See* https://fortune.com/2023/07/12/medical-giant-hca-healthcare-personal-data-11-million-patients-20-states-stolen-data-breach/ (last viewed September 17, 2023).

THE PARTIES

13. Plaintiff Sarah E. Richards is a natural person, resident, and a citizen of Denton County, in the State of Texas.

14. Plaintiff obtained healthcare from HCA through Care Now Urgent Care, located at 1017 W. Hebron Parkway, Carrolton, Texas, 75010, several times over the last several years. Plaintiff's Private Information was stored with HCA as a part of its providing healthcare services at this location.

15. To obtain healthcare services from Defendant, Plaintiff provided Defendant with highly-sensitive Private Information—including financial and health information—which was then stored on Defendant's systems.

16. Plaintiff's information was among the data accessed in the Data Breach. Plaintiff received written notice from Defendant by a letter dated August 14, 2023, sent by First Class Mail, which prompted her by hyperlink to visit a website informing Plaintiff of the HCA Healthcare facilities that may have been affected by the data breach and providing her with a toll-free number where she could call for more information about the Data Breach ("Notice").

17. Defendant obtained and continues to maintain the Private Information of Plaintiff and owed her a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed because of Defendant's inadequate data security, which resulted in the Data Breach.

18. Defendant's Notice explained the importance of protecting Private Information, and steps that Plaintiff should take to ensure the safety of her Private Information as a result of the Data Breach (Notice, ¶ What You Can Do.) Accordingly, Plaintiff spent time monitoring her credit and accounts, researching identity theft and protection options, and researched additional steps that

she should take to protect herself as a result of Defendant's wrongdoing.

19. As a result of the Data Breach, Plaintiff has experienced increased concerns, anxiety and emotional distress over the loss of privacy she experienced because of the Data Breach.

20. Further, Plaintiff has experienced anxiety and emotional distress given the increased likelihood of harm she has been exposed to because of Defendant's wrongdoing. Plaintiff has suffered imminent and impending injury arising from the substantially-increased likelihood of fraud, identity theft, and misuse of her Private Information being compromised and placed in the hands of third-party criminals.

21. Importantly, criminals steal Private Information for a reason: to misuse it later. Plaintiff's Private Information was targeted for the purpose of committing fraud. Accordingly, Plaintiff has an ongoing interest in ensuring that her information is not used for nefarious purposes.

22. Further, Plaintiff has an ongoing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

23. Defendant HCA Healthcare, Inc. is a Delaware nonprofit corporation with its principal place of business at 1 Park Plaza, in Nashville, Tennessee.

JURISDICTION AND VENUE

24. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

25. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business in the State of Tennessee and so regularly conducts business in the State of Tennessee that the Defendant is "at home" in this District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

27. HCA is one of the largest healthcare providers in the United States, operating approximately 182 hospitals and more than 2,300 sites of care, including surgery centers, freestanding ERs, urgent care centers, and physician clinics located in 20 U.S. states and in the United Kingdom.[9]

28. In addition to hospitals, HCA operates "sites of care include surgery centers, freestanding ERs, urgent care centers, diagnostic and imaging centers, walk-in clinics and physician clinics."[10]

29. Originally formed in 1968 as Hospital Corporation of America, HCA has gone through several mergers, expansions, and least two IPOs, the latest of which raised approximately $3.79 billion which was, at that time, the largest private-equity backed IPO in U.S. history.[11]

30. HCA states in bold and large font on its website: "At HCA Healthcare, we are driven by a single mission: Above all else, we are committed to the care and improvement of human life."[12]

31. HCA puts patient data right at the forefront of its pitch, acknowledging that it "analyzes data from more than 37 million patient encounters each year."[13]

---

[9] *See* HCA Healthcare website, Substitute Notice Alert, https://hcahealthcare.com/util/documents/2023/SubstituteNotice.pdf (last viewed September 17, 2023).
[10] *Id.*
[11] *See* Clare Baldwin and Alina Selyukh, "HCA IPO prices at $30, sells more shares: sources," available at https://www.reuters.com/article/us-hca-idUSTRE7280NV20110309 (last viewed September 17, 2023).
[12] *See* HCA Healthcare website, "Who We Are" https://hcahealthcare.com/about/our-mission-and-values.dot (last viewed September 17, 2023) and "Who We Are – Our Mission and Values" (last viewed September 17, 2023).
[13] *See id.,* "Who We Are" https://hcahealthcare.com/about/ (last viewed September 17, 2023).

32. Placing its collaborative and noble purposes front-and-center, HCA notes that it "provided charity care, uninsured discounts and other uncompensated care at an estimated cost of $3.3 billion in 2021."[14]

33. HCA's focus on wellbeing and collaboration places a great deal of emphasis on guaranteeing that it knows how to best care for its patients; however, in spite of these promises, HCA failed to take sufficient steps to guarantee the privacy and security of Private Information.

34. To obtain healthcare services, patients, like Plaintiff and Class Members, must provide their doctors, medical professionals, and administrators working for Defendant directly with highly sensitive Private Information. As part of their business, Defendant then compiles, stores, and maintains the Private Information they receive from patients.

35. Because of the highly sensitive and personal nature of the information Defendant acquired and stored with respect to patients and other individuals, Defendant, upon information and belief, promised to (among other things): keep PHI private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

36. As a HIPAA-covered business entity, Defendant is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI

[14] *Id.,* "Patients" https://hcahealthcareshowsup.com/home/patients.dot (last viewed September 17, 2023).

as in the case of the Data Breach complained of herein.

37. However, Defendant did not maintain adequate security to protect its systems from infiltration by cybercriminals.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

39. Defendant was in the best position to safeguard the most sensitive information it obtained from Plaintiff and Class Members. Its unique position enabled it to collect some of the most sensitive information on Plaintiff and Class Members; accordingly, Defendant had a special relationship with Plaintiff and Class Members such that they should have safeguarded that data. Defendant's website acknowledges that it, and the entities under the common ownership or control of the Defendant, are covered under the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPAA"), and HIPAA privacy rules.[15] Defendant points to the "Notice of Privacy Practices, which can be accessed at the bottom of the facility website" for how HCA treats information protected by HIPAA, but does not provide such a disclosure on its own website.[16]

40. Despite this, as part of its Privacy Policy, HCA states that "We are committed to the care and improvement of human life. Part of that commitment includes protecting your Personal

[15] *See* HCA Healthcare website, Legal, Privacy Policy, (Updated as of July 1, 2023) https://hcahealthcareshowsup.com/legal/index.dot#privacy-policy (last viewed on September 17, 2023) ("This Privacy Policy **does not apply to information that would be considered "Protected Health Information"** under the Health Insurance Portability and Accountability Act of 1996 (HIPAA"). HCA HealthCare's' use and disclosure of Protected Health Information is set forth in the HCA Healthcare **Notice of Privacy Practices,** which can be accessed at the bottom of the facility website." (emphasis in original)).

[16] *Id.*

Information (defined below). We maintain information confidentiality and comply with applicable regulatory requirements."[17]

41. These data security and privacy promises were not kept; Defendant experienced a massive data breach, and have not even provided information about how long the data breach existed before it was detected, much less an accurate picture of how many patients were implicated in the data breach.

42. The HCA Healthcare Data Breach is one of many in a long string of healthcare data breaches and, based upon information that is publicly available, should have been entirely preventable.

43. HCA's barebones notice informed victims of the Data Breach that a hacker accessed and stole files from HCA's systems, and posted samples of that information on the internet on July 5, 2023.[18]

44. HCA has offered little explanation of how patients' information was exposed in the Data Breach, stating only that hackers gained access through what appears to be "a theft from an external storage location" that was "exclusively used to automate the formatting of email messages."[19]

45. According to HCA, extensive Private Information was exfiltrated during this Data Breach, including patients' names; cities, states, and zip codes of residence; email addresses; telephone numbers; date of births; genders; patient service date and location; and next appointment date."[20]

46. HCA claims to have "reported this event to law enforcement and retained third-party

---

[17] *Id.*
[18] *See* HCA Healthcare website, Substitute Notice Alert, https://hcahealthcare.com/util/documents/2023/SubstituteNotice.pdf (last viewed September 17, 2023).
[19] *Id.*
[20] *Id.*

forensic and threat intelligence advisors."[21] HCA also stated that it "has various securities strategies, system, and protocols already in place, which are being reviewed to identify any enhancement opportunities."[22]

47. Because hackers have already infiltrated Defendant's systems, it would be easy for them to continue exploiting Defendant's systems until actual remedial measures are finalized.

HCA Is Subject to HIPAA

48. Defendant is a HIPAA covered entity that provides services to patients and healthcare and medical service providers. As a regular and necessary part of its business, Defendant collects the highly sensitive Private Information of its own patients and its clients' patients.

49. As a HIPAA covered entity, Defendant is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information they acquire, receive, and collect, and Defendant are further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

50. As a HIPAA covered entity, Defendant is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information. This includes incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

51. Defendant is in the business of providing a range of healthcare services to patients – which necessarily includes storing and maintaining electronic health records. Defendant would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

[21] *Id.*
[22] *Id.*

52. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

53. Plaintiff and Class Members are or were patients whose medical records and Private Information was maintained by Defendant and/or its affiliate hospitals, care sites, and other medical providers, who received health-related or other services from Defendant, and/or individuals who directly or indirectly entrusted Defendant with their Private Information.

54. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of their Private Information. Plaintiff and Class Members reasonably expected that Defendant would safeguard their highly sensitive information and keep that Private Information confidential.

55. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that they knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant maintained. Consequently, cybercriminals circumvented Defendant's security measures, resulting in a significant Data Breach.

The HCA Healthcare Data Breach and Notice Letter

56. According to the Notice Defendant provided to Plaintiff and Class Members, Defendant was subject to a cybersecurity ransomware attack where unauthorized parties accessed Private

Information on their networks, which was discovered on or around July 5, 2023.[23]

57. The investigation revealed that "HCA Healthcare discovered that a list of certain information with respect to some of its patients" had been stolen by unidentified unauthorized parties, containing the following types of personal information and/or protected health information: patient names; city, state, and zip code of residence; email addresses; telephone numbers; dates of birth; gender; and patient service dates, locations and next appointment dates.[24]

58. According to Defendant, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

59. Defendant claims that the information stolen in the attack did not include "Clinical information, such as treatment, diagnosis, or condition;" "Payment information, such as credit card or account numbers;" or "Sensitive information, such as passwords, driver's license or social security numbers."[25]

60. However, this is at odds with data already presented for sale on the Deep Web, where the hacker responsible for the Data Breach stated, "I have emails with health diagnosis that correspond to a clientID."[26]

61. Once HCA became aware of its Data Breach, HCA advises its clients that it "disabled user access to the storage location as an immediate containment measure," but only vaguely referenced "several robust security strategies, systems, and protocols in place to help protect data," offering no further specifics about what steps it has taken, or will take, to prevent further exploitation of

---

[23] *See* HCA Healthcare website, Substitute Notice Alert, https://hcahealthcare.com/util/documents/2023/SubstituteNotice.pdf (last viewed September 17, 2023).
[24] *Id.*
[25] *Id.*
[26] *See* Databreaches.net, https://www.databreaches.net/hca-healthcare-releases-statement-while-hacker-puts-data-up-for-sale-on-deep-web. (Last viewed September 17, 2023.)

its systems.[27]

62. As a HIPAA covered business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk which Defendant was aware of and knew it had a duty to guard against. This is particularly true because the targeted attack appears to have been a ransomware attack. It is well-known that healthcare businesses and insurers such as Defendant, which collects and stores the confidential and sensitive PII/PHI of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

63. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

64. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

65. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

66. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information

[27] *See* HCA Healthcare website, Substitute Notice Alert, https://hcahealthcare.com/util/documents/2023/SubstituteNotice.pdf (last viewed September 17, 2023).

from unauthorized disclosure.

67. Due to Defendant's inadequate security measures and their woefully inadequate notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

HCA was on Notice to the Foreseeable Risk of A Data Breach

68. As a HIPAA covered entity handling the medical patient data of insureds, Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry, and other industries holding significant amounts of PII and PHI, preceding the date of the breach.

69. At all relevant times, Defendant knew, or should have known that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that Defendant should have anticipated and guarded against.

70. Moreover, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures that would timely alert Defendant of any such attack, should one occur.

71. In light of recent high profile data breaches at other health care providers, Defendant knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

72. The rate of healthcare data breaches has been on the rise in the past five years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare

data breaches of 500 or more records were reported each day."[28]

73. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[29]

74. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

75. Indeed, cyberattacks against the healthcare industry have been common for over eleven years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[30]

---

[28] *See Healthcare Data Breach Statistics,* HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last viewed September 18, 2023).

[29] *See 2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (2022) (last viewed September 17, 2023).

[30] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://financialservices.house.gov/uploadedfiles/091411snow.pdf.

76. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[31] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[32] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[33]

77. Cyberattacks on medical systems, like Defendant's, have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[34]

78. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[35]

79. Healthcare organizations are easy targets because "even relatively small healthcare

[31] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (stating "Health information is a treasure trove for criminals.").
[32] *Id.*
[33] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.
[34] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[35] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[36] In this case, Defendant stored the records of *millions* of patients.

80. Private Information, like that stolen from Defendant, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[37]

81. Cybercriminals also maintain encrypted information on individuals to sell in "fullz"[38] records because that information can be foreseeably decrypted in the future.

82. Given these facts, any company that transacts business with consumers and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

83. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[39]

84. Defendant were on notice that the FBI has concerns about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated

---

[36] *See id.*
[37] *See id.*
[38] *See* Investopedia "Fullz (or "fulls") is a slang term for "full information." Criminals who steal credit card information use the term to refer to a complete set of information on a prospective fraud victim. https://www.investopedia.com/fullz-definition-4684000.
[39] *See* Maria Henriquez*, Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[40]

85. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[41]

86. As implied by the above AMA quote – "patient access to care" -- stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

87. The U.S. Department of Health and Human Services and the Office of Consumer Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[42]

88. As a HIPAA covered entity, Defendant should have known about their data security

---

[40] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[41] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-anagement/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[42] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in their unprotected files.

HCA Failed to Comply with FTC Guidelines

89. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

90. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[43] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[44]

91. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

92. The FTC has brought enforcement actions against businesses for failing to adequately and

[43] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[44] *Id.*

reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

93. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See*, *e.g.*, *In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

94. Defendant failed to properly implement basic data security practices, including by failing to implement an adequate intrusion detection system which would expose a breach as soon as it occurs.

95. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

96. Defendant was at all times fully aware of its obligations to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

HCA Failed to Comply with Industry Standards

97. As described above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

98. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

99. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and, training staff regarding critical points.

100. On information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

101. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

HCA's Conduct Violates HIPAA Obligations to Safeguard PII and PHI

102. As a healthcare company, and by handling medical patient data, Defendant is, and acknowledges that it is, a covered entity under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164,

Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

103. HIPAA requires a covered entity to protect against reasonably anticipated threats to the security of sensitive patient health information.

104. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

105. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

106. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

107. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

108. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

109. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Consumers Are Subject to an Increased Risk of Fraud and Identity Theft As a Result of Cyberattacks and Data Breaches

110. Cyberattacks and data breaches at health care companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

111. Researchers have found that among medical service providers that experience a data security incident, the cardiac death rate among patients increased in the months and years after the attack.[45]

112. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[46]

113. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[47]

---

[45] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[46] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[47] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

114. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

115. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[48]

116. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

117. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the

[48] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited September 17, 2023).

victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

118. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[49]

119. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

120. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

121. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

122. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

---

[49] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

123. Stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

124. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come—as Defendant has suggested that they do.

125. Private Information can sell for as much as $363 per record according to the Infosec Institute.[50] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

126. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[51] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[52] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

127. Moreover, it is no simple process to change or cancel a stolen Social Security number.

128. An individual cannot obtain a new Social Security number without significant paperwork

---

[50] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.
[51] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[52] *Id.*

and evidence of actual misuse. Even after the individual has completed the paperwork and abolished the misuse, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[53]

129. This data, as one would expect, demands a much higher price on the black market.

130. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[54]

131. Medical information is especially valuable to identity thieves.

132. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[55]

133. Legitimate companies buy PII on illegal or shadow markets in an attempt to increase their market share. Pharmaceutical makers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers do purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Additionally, Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

---

[53] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[54] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[55] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

134. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

135. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

HCA Breached Its Obligations to Plaintiff and Class Members

136. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions based upon information and belief:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);Failing to render

the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

o. Failing to adhere to industry standards for cybersecurity as discussed above; and

p. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

137. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access their computer network and systems, which contained Private Information.

138. Accordingly, as set out in detail herein, Plaintiff and Class Members are exposed to an increased risk of fraud and identity theft. And further, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant for health services.

Plaintiff Richards' and Class Members' Damages

139. Due to the heightened sensitivity of the Private Information accessed during this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not for the rest of their lives. Beyond providing inadequate credit monitoring and identify protection services, Defendant has done nothing to compensate

Plaintiff or Class Members for many of the injuries they have already suffered. Defendant has not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of its Data Breach.

140. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

141. Plaintiff's and Class Members' Private Information was all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer systems.

142. In short, once PII and PHI is exposed, there is no way to ensure that the exposed data has been fully recovered or gathered and protected against future misdeeds. Because of this, Plaintiff and Class Members will need to maintain the heightened security and monitoring measures for years, and likely for the rest of their lives due to Defendant's failures. Moreover, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

143. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

144. Due to the Data Breach, Plaintiff anticipates that she will need to spend considerable time and money on a regular and ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

145. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

146. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have

been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

147. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

148. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

149. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

150. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, and similar costs directly or indirectly related to the Data Breach.

151. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

152. Plaintiff and Class Members were also damaged by benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service—healthcare—that was intended to be accompanied by adequate data security that complied with industry standards but it was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

153. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

154. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

155. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of the Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

156. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

157. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

158. Plaintiff brings this action against Defendant on behalf of herself, individually, and on behalf of all other persons similarly situated ("the Class"), pursuant to Rule 23 of the Federal Rules of Civil Procedure.

159. Plaintiff seeks to represent a class of persons to be defined as follows, and proposes the following Class definition, subject to amendment as appropriate:

> **All persons in the United States and its territories who Defendant identified as being among those individuals impacted by the Data Breach announced on or about July 10, 2023, including all persons who were sent a notice of the Data Breach (the "Nationwide Class").**

160. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of the Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

161. This proposed class definition is based on the information available to Plaintiff at this time.

162. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses in an amended pleading or when she moves for class certification, as necessary to

account for any newly learned or changed facts as the situation develops and discovery proceeds and as this case progresses.

163. ***Numerosity.*** Plaintiff is informed and believes, and thereon alleges, that there are at a minimum, millions of members of the Class as described above. The exact size of the Class and the identities of the individual member are identifiable through HCA's records, including the files implicated in the Data Breach. The Members of the Class are so numerous that joinder of all of them is impracticable. Defendant that has acknowledged publicly that the PII of at least 11 million Class Members was compromised in Data Breach.

164. ***Commonality***. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant exercised reasonable diligence in its monitoring and HCA ,should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

165. ***Typicality***. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach and the claims of Plaintiff and the Class Members are based on the same legal theories and arise from the same unlawful and willful conduct.

166. ***Adequacy of Representation***. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Members of the Class. Plaintiff will fairly

and adequately represent and protect the interests of the Members of the Class. Plaintiff has retained Counsel who are competent and experienced in litigating class actions.

167. ***Predominance***. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, similar or identical violations, business practices, and injuries are involved. Further, all the data of Plaintiff and Class Members was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

168. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

169. ***Declaratory and Injunctive Relief Appropriate.*** Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

170. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because

such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

171. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION AND CLAIM FOR RELIEF
Negligence
(*On Behalf of Plaintiff and the Nationwide Class*)

172. Plaintiff re-alleges and incorporates by reference paragraphs 1–171 as if fully set forth

herein.

173. By collecting and storing the Private Information of Plaintiff and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duties included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

174. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

175. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

176. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

177. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the

privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

178. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

179. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

180. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place appropriate mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that

they could take appropriate steps to mitigate the potential for identity theft and other damages.

181. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendant's possession.

182. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

183. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

184. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

185. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

186. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

187. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable

result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the theft and exposure of their Private Information.

188. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and other damages as appropriate and ordered by the Court in an amount to be proven at trial.

SECOND CAUSE OF ACTION AND CLAIM FOR RELIEF
Breach of Express Contract
(On behalf of the Plaintiff and the Nationwide Class)

189. Plaintiff re-alleges and incorporates by reference paragraphs 1–171 as if fully set forth herein.

190. Defendant acquired and maintained the Private Information of Plaintiff and the Class that they received directly through Defendant's healthcare providers.

191. Defendant made express promises to Plaintiff and Class Members to safeguard their Private Information consistent with its obligation as a healthcare provider, which promises are expressly described herein.

192. Plaintiff and Class Members had agreements with Defendant under which Defendant agreed to safeguard and protect such information.

193. Plaintiff and the Class were required to deliver their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

194. Plaintiffs and Class Members were required to provide their Private Information as part of Defendant's regular business practices. Defendant accepted possession of Plaintiff's and Class

Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

195. In delivering their Private Information to Defendant and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service consistent with the express promises herein.

196. Defendant breached its express promises to safeguard Private Information with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

197. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION AND CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of the Plaintiff and the Nationwide Class)

198. Plaintiff re-alleges and incorporates by reference paragraphs 1–171 as if fully set forth herein.

199. Defendant acquired and maintained the Private Information of Plaintiff and the Class.

200. Plaintiff and the Class were required to deliver their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

201. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of their regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant, or, alternatively, provided Plaintiff's and Class Members' information to doctors or other healthcare professionals, who then provided the Private Information to Defendant.

202. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

203. In accepting such information and payment for services, Defendant entered into an implied contract with Plaintiff and the other Class Members whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

204. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Defendant and subsidiary healthcare providers.

205. In delivering their Private Information to Defendant and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard their data as part of that service.

206. The implied promise of confidentiality includes consideration beyond those pre- existing general duties owed under HIPAA or other state or federal statutes and regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

207. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve only authorized medical purposes; (3) restricting data access only to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

208. Plaintiff and the Class Members would not have entrusted their Private Information to

Defendant in the absence of such an implied contract.

209. Had Defendant disclosed to Plaintiff and the Class (or their physicians) that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Private Information to Defendant (or their physicians to provide to Defendant).

210. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

211. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

212. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

213. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION AND CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

214. Plaintiff re-alleges and incorporates by reference paragraphs 1–171 as if fully set forth herein.

215. This count for Unjust Enrichment is pleaded in the alternative to any breach of contract claim.

216. Upon information and belief, Defendant pays for its data security measures entirely from general revenue, including from money it makes based upon protecting Plaintiff's and Class Members' Private Information.

217. There is a direct nexus between money paid to Defendant and the requirement that Defendant keep Plaintiff's and Class Members' Private Information confidential and protected.

218. Plaintiff and Class Members paid Defendant and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendant.

219. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

220. Protecting data from Plaintiff and the rest of the Class Members is integral to Defendant's business. Without Class Members' data, Defendant would not be able to provide healthcare services, thus compromising Defendant's core business.

221. Plaintiff's and Class Members' data has monetary value, and Plaintiff and Class Members directly and indirectly conferred a monetary benefit on the Defendant. They indirectly conferred a monetary benefit on Defendant by purchasing goods and/or services from entities that contracted with Defendant, and from which Defendant received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendant by supplying Private Information, which has monetary value, from which value Defendant derives its business value, and which should have been protected with adequate data security.

222. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

223. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant

instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

224. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement and pay for appropriate data management and security measures that are mandated by industry standards.

225. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

226. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

227. Plaintiff and Class Members have no adequate remedy at law.

228. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to:

(i) actual identity theft;

(ii) the loss of the opportunity to determine how their Private Information is used;

(iii) the compromise, publication, and/or theft of their Private Information;

(iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

(v) lost opportunity costs associated with effort expended and the loss of

productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

(vi) the continued exposure risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession;

(vii) loss or privacy from the unauthorized access and exfiltration of their Private Information; and

(viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

229. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

230. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION AND CLAIM FOR RELIEF
Bailment
(*On Behalf of Plaintiff and the Nationwide Class*)

231. Plaintiff re-alleges and incorporates by reference paragraphs 1–171 as if set fully forth herein.

232. Plaintiff and Class Members provided Private Information to the Defendant— either directly or through subsidiary healthcare providers and their business associates—which Defendant was under a duty to keep private and confidential.

233. Plaintiff's and Class Members' Private Information is personal property, and it was conveyed to Defendant for the purpose of keeping the information private and confidential.

234. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendant was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

235. Once Defendant accepted Plaintiff's and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that Private Information once it was within the possession, custody, and control of Defendant.

236. Defendant did not safeguard Plaintiff's or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

237. Defendant's failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

238. As a result of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

SIXTH CAUSE OF ACTION AND CLAIM FOR RELIEF
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class)

239. Plaintiff re-alleges and incorporates by reference paragraphs 1–171 as if fully set forth herein.

240. In light of the special relationship between Defendant and Plaintiff and Class Members,

Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant store.

241. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with their patients to keep secure their Private Information.

242. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to protect the integrity of and monitor the activity on the systems containing Plaintiff's and Class Members' Private Information.

243. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

244. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer injury, including but not limited to:

(i) actual identity theft;

(ii) the compromise, publication, and/or theft of their Private Information;

(iii) out- of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

(iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from identity theft;

(v) the continued exposure risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

(vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

(vii) the diminished value of Defendant's services they received.

245. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff Richards as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five years of credit monitoring and identify theft services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, statutory penalties, and other damages the Court deems appropriate, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and,

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: September 20, 2023

Respectfully Submitted,

/s/J. Gerard Stranch, IV

J. Gerard Stranch, IV (BPR 23045)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue
Suite 200
Nashville, TN 37203
Tel: 615.254.8801
gstranch@stranchlaw.com

Ariana J. Tadler, Esq.*
A.J. de Bartolomeo, Esq.*
TADLER LAW LLP
22 Bayview Avenue, Suite 200
Manhasset, NY 11030
Tel: 212.946.9300

atadler@tadlerlaw.com
ajd@tadlerlaw.com

* *Pro Have Vice Forthcoming*

Counsel for Plaintiff Sarah E. Richards